UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/943,822 | 08/31/2001 | Michael Gill | 1662-40200 (P00-3357) | 1422 |

23505 7590 06/17/2005

CONLEY ROSE, P.C.
P. O. BOX 3267
HOUSTON, TX 77253-3267

| EXAMINER | |
|---|---|
| REVAK, CHRISTOPHER A | |
| **ART UNIT** | **PAPER NUMBER** |
| 2131 | |

DATE MAILED: 06/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/943,822 | GILL ET AL. | |
| | Examiner | Art Unit | |
| | Christopher A. Revak | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *31 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1,2,4,6-8,11-16,19,20,22-24,27-32, and 35-37 are rejected under 35 U.S.C. 102(e) as being anticipated by Burns et al, U.S. Patent 6,405,315.

As per claims 1 and 19, the teachings of Burns et al disclose of a method and system for transferring data between a client (computer) and a storage device which are both connected across a network. The data is encrypted by a client (computer) and then transmitted across a network to the storage device where it is then stored on the storage device (col. 3, lines 10-24). The examiner is interpreting the storage device of Burns et al to be that of non-volatile since non-volatile is used for storing data that does not lose the data when power is removed from the device.

As per claims 2 and 20, it is disclosed by Burns et al that a header is created containing the destination information pertaining to the storage device and transmitting the encrypted data with the header (col. 6, lines 21-33 & 38-41).

As per claim 4, the teachings of Burns et al disclose of the use of a header used in a network protocol such as an Ethernet (col. 6, lines 21-33 & 38-41) and it is interpreted by the examiner that the header is removed prior to storing the encrypted data on the storage device because a feature of protocols is to contain information that is appended to the contents, or packets, such as destination and source address, error checking codes so that the information is properly received and various other fields and upon acceptance, that information is then discarded.

As per claims 6 and 22, the teachings of Burns et al disclose of retrieving the encrypted data from the storage device and transmitting the encrypted data to the client (computer)(col. 3, lines 25-47).

As per claims 7 and 23, the teachings of Burns et al disclose of receiving the encrypted data at the client (computer) and decrypting the received encrypted data (col. 3, lines 16-20).

As per claims 8 and 24, Burns et al disclose of transmitting the encrypted data to the client (computer) with a header that provides routing information pertaining to the client (computer)(col. 6, lines 21-33 & 38-41).

As per claims 11 and 27, the teachings of Burns et al disclose of a method and system for transferring data between a client (computer) and a storage device which are both connected across a network. The encrypted data is retrieved from the storage device and transmitted across the network from the storage device to the client (computer). The encrypted data is received by the client (computer) and then is decrypted (col. 3, lines 10-24 & 25-47). The examiner is interpreting the storage device

of Burns et al to be that of non-volatile since non-volatile is used for storing data that does not lose the data when power is removed from the device.

As per claims 12 and 28, Burns et al disclose of transmitting the encrypted data to the client (computer) with a header that provides routing information pertaining to the client (computer)(col. 6, lines 21-33 & 38-41).

As per claims 13 and 29, the teachings of Burns et al disclose of receiving the encrypted data at the client (computer) and decrypting the received encrypted data (col. 3, lines 16-20). The teachings of Burns et al disclose of the use of a header used in a network protocol such as an Ethernet (col. 6, lines 21-33 & 38-41) and it is interpreted by the examiner that the header is removed prior to storing the encrypted data on the storage device because a feature of protocols is to contain information that is appended to the contents, or packets, such as destination and source address, error checking codes so that the information is properly received and various other fields and upon acceptance, that information is then discarded.

As per claims 14 and 30, Burns et al discloses of the data is encrypted by a client (computer) and then transmitted across a network to the storage device where it is then stored on the storage device (col. 3, lines 10-24).

As per claims 15 and 31, it is disclosed by Burns et al that a header is created containing the destination information pertaining to the storage device and transmitting the encrypted data with the header (col. 6, lines 21-33 & 38-41).

As per claims 16 and 32, the teachings of Burns et al disclose of the use of a header used in a network protocol such as an Ethernet (col. 6, lines 21-33 & 38-41) and

it is interpreted by the examiner that the header is removed prior to storing the encrypted data on the storage device because a feature of protocols is to contain information that is appended to the contents, or packets, such as destination and source address, error checking codes so that the information is properly received and various other fields and upon acceptance, that information is then discarded.

As per claim 35, the teachings of Burns et al disclose of a method for transferring data between a client (computer) and a storage device which are both connected across a network. The client initiates a command for data and it is then encrypted by a client (computer) for transmission across a network to the storage device where it is then stored on the storage device (col. 3, lines 10-25). The examiner is interpreting the storage device of Burns et al to be that of non-volatile since non-volatile is used for storing data that does not lose the data when power is removed from the device.

As per claim 36, it is disclosed by Burns et al of encrypting data by a client (computer) with a (dynamically generated session) key for transmission across a network to the storage device where it is then stored on the storage device (col. 3, lines 10-25 & 35-39).

As per claim 37, the teachings of Burns et al disclose of receiving the encrypted data at the client (computer) and decrypting the received encrypted data with a (dynamically generated session) key (col. 3, lines 16-20 & 35-39).

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 3,5, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burns et al, U.S. Patent 6,405,315 in view of Collins et al, U.S. Patent 6,378,072.

As per claims 3,5, and 21, the teachings of Burns et al discloses of a header that is created containing the destination information pertaining to the storage device and transmitting the encrypted data with the header (col. 6, lines 21-33 & 38-41). The teachings of Burns et al are silent in disclosing of the header containing cryptographic metrics for the data and using the cryptographic metrics to validate the integrity/authenticity of the data prior to taking action on the data. The teachings of Collins et al disclose of header containing a digital signature (cryptographic metrics) for the data and using the digital signature (cryptographic metrics) to validate the integrity/authenticity of the data prior to taking action on the data (col. 2, lines 48-52 & 60-64). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply means to check for the integrity and authenticity of data items. Collins et al recites motivation for the use of digital signatures by disclosing that application programs can't be maliciously altered or changed with fraudulent programs (col. 3, lines 8-9). The teachings of Burns et al are concerned with securely storing data on network storage devices and it is obvious that

the teachings of Collins et al offer further measures to ensure the secure storage of data by using digital signatures to ensure the integrity and authenticity of the data.

5. Claims 9,10,17,18,25,26,33, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burns et al, U.S. Patent 6,405,315 in view of Downs et al, U.S. Patent 6,226,618.

The teachings of Burns et al disclose of the transmission of encrypted data from a client to a storage device wherein the storage device returns encrypted data back to the client for decryption (col. 3, lines 10-24 & 25-47). The teachings of Burns et al are silent in the use of encrypting the encrypted data with a predetermined key and transmitting the twice encrypted data. It is disclosed by Downs et al of twice encrypting data with a predetermined key (col. 3, lines 42-46). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply dual encryption layers to further protect data. The teachings of Downs et al recite of motivation for the use of twice encrypted data by disclosing of the need for secure delivery and rights management for digital data and the need to ensure the protection and security of that information that is distributed electronically (col. 1, lines 52-57 and col. 2, lines 24-25). In that the teachings of Burns et al are concerned with securely storing data on network storage devices, Downs et al offers further protection by twice encrypting data for further protection and it is obvious that the teachings of Burns et al would have been more secure against unauthorized parties trying to access data since it is encrypted twice.

***Conclusion***

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Pham et al, U.S. Patent 6,678,828 discloses of encryption of data files that are transmitted across a network and stored on network storage devices.

Fransdonk, WO 01/98903 discloses of storing encrypted contents at a third party location wherein the data is twice encrypted.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

CR

June 10, 2005